IN THE SPECIFICATION:

Please amend the title as follows:

- - NON MALLEABLE ENCRYPTION METHOD AND APPARATUS USING KEY-ENCRYPTION KEYS AND DIGITAL SIGNATURE ~~ENCRYPTION AND SIGNATURE METHOD AND APPARATUS~~ - -

Please amend the specification as follows:

p. 9, third paragraph – pg. 10, first paragraph:

B1

Encryption methods, other than ElGamal can be used, particularly variations of ElGamal. Signature methods other than Schnorr can be used such as Digital Signature Standard (hereinafter "DSS") which is a U.S. signature standard. Instead of a signature method, a proof-of-discrete-log system can be used. Several such methods are well known in the literature.

The Schnorr signature process uses one or both portions (a, b) of the standard ElGamal encryption as a public key, most likely just the portion 'b' of the standard ElGamal encryption and the corresponding secret portion (the random number 'c' above), to sign a message. A signature 's' is provided with the encrypted message. The signature 's' is a function of the encrypted message (a, b), potentially including publicly available information, such as the time or date. It can be publicly verified by anybody who gets the ciphertext, but can only be generated by a party with knowledge of the secret random number "c" used for encryption ~~used for encryption~~. In the example referred to, the signer's secret key is based on the random number "c" which is used by the entity or processor, such as encryption processor 12, which encrypts a message, such as message "m", and said encryption processor also preferably functions as a signing processor 16 which computes the ciphertext (a,b,s). The overall encryption data is now a triplet of (a,b,s). In this case (a,b) or portions thereof act as the public key, (a,b) or a function thereof is the message

and "s" is the signature. The ciphertext (referring to (a,b, and s)) is said to be valid if "s" is the signature on (a,b) with respect to the chosen public key (which is (a,b, or functions of these)).